

EXPLICIT EVALUATION OF DOUBLE GAUSS SUMS

ŞABAN ALACA AND GREG DOYLE

ABSTRACT. We present an explicit evaluation of the double Gauss sum

$$G(a, b, c; S; p^n) := \sum_{x, y=0}^{p^n-1} e^{2\pi i S(ax^2 + bxy + cy^2)/p^n},$$

where a, b, c are integers such that $\gcd(a, b, c) = 1$, p is a prime, n is a positive integer, and S is an integer coprime to p .

Key words and phrases: Gauss sums; double Gauss sums; exponential sums; binary quadratic forms; quadratic exponential sums.

2010 Mathematics Subject Classification: 11L03, 11L05, 11T23, 11E16, 11E25, 11D79.

1. INTRODUCTION

We let \mathbb{N} denote the set of positive integers, \mathbb{N}_0 the non-negative integers, \mathbb{Z} the integers, \mathbb{Q} the rational numbers and \mathbb{C} the complex numbers. Let $a, b, c, S \in \mathbb{Z}$, $n \in \mathbb{N}$ and let p be a prime. For convenience we set $e(\alpha) := e^{2\pi i \alpha}$ for any $\alpha \in \mathbb{Q}$.

The (quadratic) Gauss sum $G(S; p^n)$ is defined by

$$(1.1) \quad G(S; p^n) := \sum_{x=0}^{p^n-1} e\left(\frac{Sx^2}{p^n}\right).$$

The evaluation of $G(S; p^n)$ is well known and was first determined by Gauss [4]. In this paper we evaluate a similar sum with binary quadratic form argument.

We define the double (quadratic) Gauss sum $G(a, b, c; S; p^n)$ by

$$(1.2) \quad G(a, b, c; S; p^n) := \sum_{x, y=0}^{p^n-1} e\left(\frac{S(ax^2 + bxy + cy^2)}{p^n}\right).$$

If $p^n \mid S$ then we have

$$(1.3) \quad G(S; p^n) = \sum_{x=0}^{p^n-1} 1 = p^n \quad \text{and} \quad G(a, b, c; S; p^n) = \sum_{x, y=0}^{p^n-1} 1 = p^{2n}.$$

If $p^n \nmid S$ then $p^m \parallel S$ for some $m \in \mathbb{N}_0$ with $m < n$, so that $S_1 = S/p^m \in \mathbb{Z}$, and

$$(1.4) \quad \begin{aligned} G(S; p^n) &= \sum_{x=0}^{p^n-1} e\left(\frac{Sx^2}{p^n}\right) = \sum_{x=0}^{p^n-1} e\left(\frac{S_1x^2}{p^{n-m}}\right) \\ &= p^m \sum_{x=0}^{p^{n-m}-1} e\left(\frac{S_1x^2}{p^{n-m}}\right) = p^m G(S_1; p^{n-m}) \end{aligned}$$

and

$$(1.5) \quad \begin{aligned} G(a, b, c; S; p^n) &= \sum_{x,y=0}^{p^n-1} e\left(\frac{S(ax^2 + bxy + cy^2)}{p^n}\right) = \sum_{x,y=0}^{p^n-1} e\left(\frac{S_1(ax^2 + bxy + cy^2)}{p^{n-m}}\right) \\ &= p^{2m} \sum_{x,y=0}^{p^{n-m}-1} e\left(\frac{S_1(ax^2 + bxy + cy^2)}{p^{n-m}}\right) \\ &= p^{2m} G(a, b, c; S_1; p^{n-m}). \end{aligned}$$

Thus we may assume that S is coprime to p and $\gcd(a, b, c) = 1$. We write (a, b, c) to denote $\gcd(a, b, c)$. The sum $G(a, b, c; S; p^n)$ was first evaluated by Weber [6] for b even, and subsequently refined by Jordan [5] around 1870. Alaca, Alaca and Williams [1] evaluated the sum $G(a, b, c; S; p^n)$ given the condition $4ac - b^2 \neq 0$. In each of these papers, the main idea is to use a linear change of variables to diagonalize the binary quadratic form

$$(1.6) \quad Q := Q(x, y) = ax^2 + bxy + cy^2.$$

In this fashion, if $Q \sim Q' = Ax^2 + Cy^2$ for some integers A and C , then

$$(1.7) \quad G(Q; S; p^n) = G(Q'; S; p^n) = G(AS; p^n) \cdot G(CS; p^n).$$

Our approach is similar to those earlier ideas, but our choice for change of variables will generalize those results in an explicit fashion. Our approach differs from the approach of Weber [6] and Jordan [5], who diagonalized Q recursively. We first evaluate $G(a, b, c; S; p^n)$ for p an odd prime, and subsequently $G(a, b, c; S; 2^n)$. It should be noted that references to the papers [6] and [5] are rare. As those papers were written in German and French, respectively, this paper may also serve as a modern translation of those ideas.

We may assume that $a, b \neq 0$, and permuting coefficients if necessary, we may also assume that if $p^m \parallel a$ for some $m \in \mathbb{N}$, then $p^m \mid c$. We observe that

$$(1.8) \quad G(a, b, c; S; p^n) = G(\bar{a}, \bar{b}, \bar{c}; S; p^n),$$

where \bar{a} , \bar{b} and \bar{c} denote the residue classes of a , b and c modulo p^n , respectively. Hence, we may identify a, b and c with their positive integer residues modulo p^n .

We write $a \equiv p^\alpha A \pmod{p^n}$ and $b \equiv p^\beta B \pmod{p^n}$, where $\alpha, \beta \in \mathbb{N}_0$ and $A, B \in \mathbb{Z}$ satisfy $p \nmid AB$. Thus, we may assume that a, b and c are of the form

$$(1.9) \quad (a, b, c) = 1, \quad a \equiv p^\alpha A \pmod{p^n}, \quad b \equiv p^\beta B \pmod{p^n}, \quad c \equiv 0 \pmod{p^\alpha},$$

where $A, B \in \mathbb{Z}$ satisfy $p \nmid AB$, and $\alpha, \beta \in \mathbb{N}_0$. We note that (1.9) implies that at least one of α, β is zero. We use the inequality $\alpha \leq \beta$ to indicate that $\alpha = 0$, and similarly we use $\beta \leq \alpha$ to indicate that $\beta = 0$. Finally, the discriminant of the binary quadratic form Q in (1.6) is defined by $\Delta := 4ac - b^2$.

2. PRELIMINARY RESULTS FOR GAUSS SUMS

For the remainder of the paper, we let $\left(\frac{S}{p}\right)$ denote the Jacobi-Kronecker-Legendre symbol. The following theorem is the famous deep formula first given by Gauss [4]. One can consult the excellent monograph by Berndt, Evans and Williams [2, pp. 18-28] for an elementary proof.

Theorem 2.1. *Let $k \in \mathbb{N}$. For $S \in \mathbb{Z}$ coprime to k , we have*

$$G(S; k) := \sum_{x=0}^{k-1} e\left(\frac{Sx^2}{k}\right) = \begin{cases} \left(\frac{S}{k}\right) \sqrt{k} & \text{if } k \equiv 1 \pmod{4} \\ 0 & \text{if } k \equiv 2 \pmod{4} \\ \left(\frac{S}{k}\right) \sqrt{-k} & \text{if } k \equiv 3 \pmod{4} \\ \left(\frac{k}{S}\right) (1 + i^S) \sqrt{k} & \text{if } k \equiv 0 \pmod{4}. \end{cases}$$

The following corollary is a special case of Theorem 2.1 for $k = p^n$.

Corollary 2.1. *Let p be a prime, $n \in \mathbb{N}$ and $S \in \mathbb{Z}$ coprime to p .*

If p is odd, we have

$$G(S; p^n) = i^{\left(\frac{p^n-1}{2}\right)^2} \left(\frac{S}{p}\right)^n \sqrt{p^n}.$$

If $p = 2$, we have

$$G(S; 2^n) = \begin{cases} 0 & \text{if } n = 1 \\ (1 + i^S) \left(\frac{2}{S}\right)^n \sqrt{2^n} & \text{if } n > 1. \end{cases}$$

We now prove some basic results for the Gauss sum (1.1) and for its variations.

Lemma 2.1. *Let p be a prime, $n \in \mathbb{N}$ and $S \in \mathbb{Z}$ be coprime to p . We identify S^{-1} with the least positive integer residue of the inverse of S modulo p^n . Then we have*

$$G(S^{-1}; p^n) = G(S; p^n) \text{ and } G(S^2; p^n) = G(1; p^n).$$

Proof. We first suppose that p is odd. By Corollary 2.1, we have

$$G(S^2; p^n) = \left(\frac{S^2}{p}\right)^n i^{\left(\frac{p^n-1}{2}\right)^2} \sqrt{p^n} = G(1; p^n).$$

As $\left(\frac{S^{-1}}{p}\right) = \left(\frac{S^2}{p}\right) \left(\frac{S^{-1}}{p}\right) = \left(\frac{S}{p}\right)$, Corollary 2.1 yields $G(S^{-1}; p^n) = G(S; p^n)$.

We now suppose that $p = 2$. If $n = 1$, then we have $G(S; 2) = 0 = G(S^{-1}; 2)$. We assume that $n \geq 2$. As S is odd, we have $S^2 \equiv 1 \pmod{8}$, which implies that $S^{-1} \equiv 1 \pmod{8}$ so that $\left(\frac{2}{S^{-1}}\right) = \left(\frac{2}{S}\right)$ and further that $i^{S^{-1}} = i^S$, so by Corollary 2.1, we have $G(S^{-1}; 2^n) = G(S; 2^n)$. By similar reasoning, one can see that $G(S^2; 2^n) = G(1; 2^n)$. \square

Lemma 2.2. *Let p be a prime, $n \in \mathbb{N}$ and $S \in \mathbb{Z}$ coprime to p . Let $\alpha, \beta \in \mathbb{N}_0$ satisfy $\alpha, \beta \leq n$.*

If p is odd, we have

$$\sum_{\substack{x=0 \\ x \equiv 0 \pmod{p^\alpha}}}^{p^n-1} e\left(\frac{Sp^\beta x^2}{p^n}\right) = \begin{cases} p^{n-\alpha} & \text{if } 2\alpha + \beta \geq n \\ p^\beta \cdot G(S; p^{n-\beta}) & \text{if } 2\alpha + \beta \leq n. \end{cases}$$

If $p = 2$, we have

$$\sum_{\substack{x=0 \\ x \equiv 0 \pmod{2^\alpha}}}^{2^n-1} e\left(\frac{S2^\beta x^2}{2^n}\right) = \begin{cases} 2^{n-\alpha} & \text{if } 2\alpha + \beta \geq n \\ 0 & \text{if } 2\alpha + \beta = n - 1 \\ 2^\beta \cdot G(S; 2^{n-\beta}) & \text{if } 2\alpha + \beta \leq n - 2. \end{cases}$$

Proof. We first suppose that p is odd. As $\alpha \leq n$, we have

$$(2.1) \quad \sum_{\substack{x=0 \\ x \equiv 0 \pmod{p^\alpha}}}^{p^n-1} e\left(\frac{Sp^\beta x^2}{p^n}\right) = \sum_{x=0}^{p^{n-\alpha}-1} e\left(\frac{Sp^{\alpha+\beta} x^2}{p^{n-\alpha}}\right) = G(Sp^{\alpha+\beta}; p^{n-\alpha}).$$

If $2\alpha + \beta \geq n$, we see that (2.1) simplifies to $p^{n-\alpha}$. If $2\alpha + \beta \leq n$, by (1.4) and Corollary 2.1, we have

$$G(Sp^{\alpha+\beta}; p^{n-\alpha}) = p^{\alpha+\beta} \cdot G(S; p^{n-\beta-2\alpha}) = p^\beta \cdot G(S; p^{n-\beta}),$$

where we have used the fact that $p^{n-\beta-2\alpha} \equiv p^{n-\beta} \pmod{4}$. We have similar reasoning for $p = 2$, with the exception that if $2\alpha + \beta = n - 1$ then, by (1.4) and Corollary 2.1, we have $G(S2^{\alpha+\beta}; 2^{n-\alpha}) = 0$. \square

Note that if p is odd and $2\alpha + \beta = n$ then both statements of Lemma 2.2 agree. Indeed, under this assumption, we see from Corollary 2.1 that

$$p^\beta \cdot G(S; p^{n-\beta}) = p^{n-2\alpha} \cdot G(S; p^{2\alpha}) = p^{n-\alpha}.$$

We emphasize that the following proof of Lemma 2.3 is clearly modeled after the proof of Lemma 3.1 [1, pp. 145-147] in the paper by Alaca, et al.

Lemma 2.3. *Let p be a prime, $n \in \mathbb{N}$, $w \in \mathbb{Z}$ and $S \in \mathbb{Z}$ coprime to p . Let $\alpha, \beta \in \mathbb{N}_0$ satisfy $\alpha, \beta \leq n$.*

If p is odd and $2\alpha + \beta \leq n$, we have

$$\sum_{\substack{x=0 \\ x \equiv w \pmod{p^\alpha}}}^{p^n-1} e\left(\frac{Sp^\beta x^2}{p^n}\right) = \begin{cases} 0 & \text{if } w \not\equiv 0 \pmod{p^\alpha} \\ p^\beta \cdot G(S; p^{n-\beta}) & \text{if } w \equiv 0 \pmod{p^\alpha}. \end{cases}$$

If $p = 2$ and $2\alpha + \beta \leq n - 2$, we have

$$\sum_{\substack{x=0 \\ x \equiv w \pmod{2^\alpha}}}^{2^n-1} e\left(\frac{S2^\beta x^2}{2^n}\right) = \begin{cases} 0 & \text{if } w \not\equiv 0 \pmod{2^\alpha} \\ 2^\beta \cdot G(S; 2^{n-\beta}) & \text{if } w \equiv 0 \pmod{2^\alpha}. \end{cases}$$

Proof. We first suppose that p is odd and $2\alpha + \beta \leq n$. If $w \equiv 0 \pmod{p^\alpha}$, the statement of the lemma is given by Lemma 2.2 and so we may assume that $p^\alpha \nmid w$. We have

$$\begin{aligned} \sum_{\substack{x=0 \\ x \equiv w \pmod{p^\alpha}}}^{p^n-1} e\left(\frac{Sp^\beta x^2}{p^n}\right) &= \frac{1}{p^\alpha} \sum_{x=0}^{p^n-1} e\left(\frac{Sx^2}{p^{n-\beta}}\right) \sum_{y=0}^{p^\alpha-1} e\left(\frac{(x-w)y}{p^\alpha}\right) \\ &= \frac{1}{p^\alpha} \sum_{y=0}^{p^\alpha-1} e\left(\frac{-wy}{p^\alpha}\right) \sum_{x=0}^{p^n-1} e\left(\frac{Sx^2}{p^{n-\beta}} + \frac{xy}{p^\alpha}\right) \\ (2.2) \quad &= \frac{p^\beta}{p^\alpha} \sum_{y=0}^{p^\alpha-1} e\left(\frac{-wy}{p^\alpha}\right) \sum_{x=0}^{p^{n-\beta}-1} e\left(\frac{Sx^2 + xyp^{n-\alpha-\beta}}{p^{n-\beta}}\right), \end{aligned}$$

where we have used (1.4) to extract p^β . Observe that as $2\alpha + \beta \leq n$, we have $(p^{n-\alpha-\beta})^2 \equiv 0 \pmod{p^{n-\beta}}$. By completing the square modulo $p^{n-\beta}$ we obtain

$$(2.3) \quad Sx^2 + p^{n-\alpha-\beta}xy \equiv S(x + (2S)^{-1}p^{n-\alpha-\beta}xy)^2 \pmod{p^{n-\beta}}.$$

As x runs over a complete residue system modulo $p^{n-\beta}$, so does the bracketed expression in (2.3). Thus, (2.2) simplifies to

$$(2.4) \quad \sum_{\substack{x=0 \\ x \equiv w \pmod{p^\alpha}}}^{p^n-1} e\left(\frac{Sp^\beta x^2}{p^n}\right) = \frac{p^\beta}{p^\alpha} \cdot G(S; p^{n-\beta}) \sum_{y=0}^{p^\alpha-1} e\left(\frac{-wy}{p^\alpha}\right).$$

The innermost sum of (2.4) is a geometric sum. As $w \not\equiv 0 \pmod{p^\alpha}$, the right-hand side of (2.4) will reduce to zero, which completes the first part of the lemma.

We now suppose that $p = 2$ and $2\alpha + \beta \leq n - 2$. We proceed in a similar manner as in the odd prime case to arrive at

$$(2.5) \quad \sum_{\substack{x=0 \\ x \equiv w \pmod{2^\alpha}}}^{2^n-1} e\left(\frac{Sx^2}{2^n}\right) = \frac{2^\beta}{2^\alpha} \sum_{y=0}^{2^\alpha-1} e\left(\frac{-wy}{2^\alpha}\right) \sum_{x=0}^{2^{n-\beta}-1} e\left(\frac{Sx^2 + 2^{n-\alpha-\beta}xy}{2^{n-\beta}}\right).$$

As $2\alpha + \beta \leq n - 2$, we have $(2^{n-\alpha-\beta-1})^2 \equiv 0 \pmod{2^{n-\beta}}$. Completing the square as before, we obtain

$$(2.6) \quad Sx^2 + 2^{n-\alpha-\beta}xy \equiv S(x + S^{-1}2^{n-\alpha-\beta-1}y)^2 \pmod{2^{n-\beta}}.$$

Hence, with (2.6) we see that (2.5) simplifies to

$$\sum_{\substack{x=0 \\ x \equiv w \pmod{2^\alpha}}}^{2^n-1} e\left(\frac{Sx^2}{2^n}\right) = \frac{2^\beta}{2^\alpha} \cdot G(S; 2^{n-\beta}) \sum_{y=0}^{2^\alpha-1} e\left(\frac{-wy}{2^\alpha}\right),$$

which simplifies to the second part of the lemma. \square

Lemma 2.4. *Let p be a prime, $n \in \mathbb{N}$, $w \in \mathbb{Z}$ and $S \in \mathbb{Z}$ coprime to p . Let $\alpha, \beta \in \mathbb{N}_0$ satisfy $\alpha, \beta \leq n$.*

If p is odd and $2\alpha + \beta \leq n$, we have

$$\sum_{x=0}^{p^n-1} e\left(\frac{Sp^\beta(p^\alpha x + w)^2}{p^n}\right) = \begin{cases} 0 & \text{if } w \not\equiv 0 \pmod{p^\alpha} \\ p^{\alpha+\beta} \cdot G(S; p^{n-\beta}) & \text{if } w \equiv 0 \pmod{p^\alpha} \end{cases}.$$

If $p = 2$ and $2\alpha + \beta \leq n - 2$, we have

$$\sum_{x=0}^{2^n-1} e\left(\frac{S2^\beta(2^\alpha x + w)^2}{2^n}\right) = \begin{cases} 0 & \text{if } w \not\equiv 0 \pmod{2^\alpha} \\ 2^{\alpha+\beta} \cdot G(S; 2^{n-\beta}) & \text{if } w \equiv 0 \pmod{2^\alpha} \end{cases}.$$

Proof. For any prime p , from (1.4) we have

$$\sum_{x=0}^{p^n-1} e\left(\frac{Sp^\beta(p^\alpha x + w)^2}{p^n}\right) = p^\beta \sum_{x=0}^{p^{n-\beta}-1} e\left(\frac{S(p^\alpha x + w)^2}{p^{n-\beta}}\right).$$

Hence, we may replace n by $n - \beta$ in the statements of the lemma to arrive at the same result. Thus, we may suppose that $\beta = 0$. We have

$$(2.7) \quad \sum_{x=0}^{p^n-1} e\left(\frac{S(p^\alpha x + w)^2}{p^n}\right) = \sum_{\substack{x=0 \\ x \equiv w \pmod{p^\alpha}}}^{p^{n+\alpha}-1} e\left(\frac{Sx^2}{p^n}\right) = p^\alpha \sum_{\substack{x=0 \\ x \equiv w \pmod{p^\alpha}}}^{p^n-1} e\left(\frac{Sx^2}{p^n}\right).$$

The assertions of the lemma follow by considering the parity of p in (2.7) with respect to Lemma 2.3. \square

We now prove a simple result regarding the double gauss sum $G(a, b, c; S; p^n)$.

Lemma 2.5. *Let p be a prime, $n \in \mathbb{N}$ and $S \in \mathbb{Z}$ coprime to p . Let $b \in \mathbb{Z}$ and write $b \equiv p^\beta B \pmod{p^n}$ for $\beta \in \mathbb{N}_0$ and $B \in \mathbb{Z}$ coprime to p . Then we have*

$$G(0, b, 0; S; p^n) = p^{n+\beta}.$$

Proof. We have

$$(2.8) \quad G(0, b, 0; S; p^n) = \sum_{x,y=0}^{p^n-1} e\left(\frac{p^\beta Bxy}{p^n}\right).$$

The result is clear when $\beta = n$ and so we may assume that $\beta < n$. Along with (1.5), the expression for $G(0, b, 0; S; p^n)$ in (2.8) will simplify to

$$p^{2\beta} \sum_{x,y=0}^{p^{n-\beta}-1} e\left(\frac{Bxy}{p^{n-\beta}}\right) = p^{2\beta} \left[p^{n-\beta} + \sum_{y=1}^{p^{n-\beta}-1} \sum_{x=0}^{p^{n-\beta}-1} e\left(\frac{Bxy}{p^{n-\beta}}\right) \right] = p^{n+\beta},$$

which completes the proof. \square

We now diagonalize our binary quadratic form Q given in (1.6).

Theorem 2.2. *Let Q be the binary quadratic form given in (1.6). If $a \neq 0$, we have*

$$(2.9) \quad 4a \cdot Q = (2ax + by)^2 + \Delta y^2.$$

Proof. Let $M := \begin{pmatrix} 2a & b \\ b & 2c \end{pmatrix}$. Then $Q = [x \ y] \frac{M}{2} [x \ y]^T$. As $a \neq 0$, we can express the matrix M as $M = LDL^T$, where $L = \begin{pmatrix} 1 & 0 \\ \frac{b}{2a} & 1 \end{pmatrix}$ and $D = \begin{pmatrix} 2a & 0 \\ 0 & \frac{\Delta}{2a} \end{pmatrix}$. Therefore, we have

$$(2.10) \quad Q = [x \ y] L \frac{D}{2} L^T [x \ y]^T = ([x \ y] L) \frac{D}{2} ([x \ y] L)^T.$$

Let $X_1 := x + \frac{b}{2a}y$ and $X_2 := y$ denote the change of variables given by L . We substitute this into (2.10) to obtain

$$Q = [X_1 \ X_2] \frac{D}{2} [X_1 \ X_2]^T = aX_1^2 + \frac{\Delta}{4a}X_2^2 = \frac{1}{4a}(2aX_1)^2 + \frac{\Delta}{4a}X_2^2,$$

which completes the proof. \square

Note that one can easily expand the square and collect like terms in (2.9) to show equality. Our LDL^T diagonalization method would generalize to a quadratic form in n variables, with a certain non-singularity condition. It's well known that any integral quadratic form is equivalent to a diagonal quadratic form with rational coefficients [3, pp. 69-70], and so our method may work for other diagonalizations of Q .

We look at the equation in (2.9) modulo a prime power. Allowing for the divisibility of $4a$, one can deduce the following corollary from Theorem 2.2.

Corollary 2.2. *Let Q be the quadratic form given in (1.6) and suppose $a \neq 0$. Let p be a prime and $n \in \mathbb{N}$. We write $a = p^\alpha A$ for $\alpha \in \mathbb{N}_0$ and $A \in \mathbb{Z}$ coprime to p .*

If p is odd, we have

$$p^\alpha \cdot Q \equiv (4A)^{-1}(2Ap^\alpha x + by)^2 + (4A)^{-1}\Delta y^2 \pmod{p^{n+\alpha}}.$$

If $p = 2$, we have

$$2^{\alpha+2} \cdot Q \equiv A^{-1}(2^{\alpha+1}Ax + by)^2 + A^{-1}\Delta y^2 \pmod{2^{n+\alpha+2}}.$$

3. EXPLICIT EVALUATION OF DOUBLE GAUSS SUMS

Theorem 3.1. *Let p be a prime, $n \in \mathbb{N}$, $S \in \mathbb{Z}$ coprime to p and let $a, b, c \in \mathbb{Z}$ be as in (1.9), namely*

$$(a, b, c) = 1, \quad a \equiv p^\alpha A \pmod{p^n}, \quad b \equiv p^\beta B \pmod{p^n}, \quad c \equiv 0 \pmod{p^\alpha},$$

where $A, B \in \mathbb{Z}$ satisfy $p \nmid AB$, and $\alpha, \beta \in \mathbb{N}_0$. Note that if $p^n \mid a$, then by convention we set $\alpha = n$ and $A = 1$. We set $\Delta := 4ac - b^2$.

If p is odd, we have

$$G(a, b, c; S; p^n) = G(SA; p^{n-\alpha}) \cdot G(SA\Delta; p^{n+\alpha}).$$

If $p = 2$, we have

$$G(a, b, c; S; 2^n) = \begin{cases} \frac{1}{4} \cdot G(SA; 2^{n-\alpha}) \cdot G(SA\Delta; 2^{n+\alpha+2}) & \text{if } \alpha + 1 < n \\ (-1)^c(1 + (-1)^{b+1}) & \text{if } \alpha + 1 \geq n = 1 \\ 2^n & \text{if } \alpha + 1 \geq n > 1. \end{cases}$$

Proof. We first suppose that p is odd. By (1.2), (1.5) and Corollary 2.2, we have

$$\begin{aligned} G(a, b, c; S; p^n) &= \frac{1}{p^{2\alpha}} G(a, b, c; Sp^\alpha; p^{n+\alpha}) \\ &= \frac{1}{p^{2\alpha}} \sum_{x, y=0}^{p^{n+\alpha}-1} e\left(\frac{S((4A)^{-1}(2Ap^\alpha x + by)^2 + (4A)^{-1}\Delta y^2)}{p^{n+\alpha}}\right) \\ (3.1) \quad &= \frac{1}{p^{2\alpha}} \sum_{y=0}^{p^{n+\alpha}-1} e\left(\frac{S(4A)^{-1}\Delta y^2}{p^{n+\alpha}}\right) \sum_{x=0}^{p^{n+\alpha}-1} e\left(\frac{S(4A)^{-1}(2Ap^\alpha x + p^\beta By)^2}{p^{n+\alpha}}\right). \end{aligned}$$

Assume that $\alpha \leq \beta$. We have

$$2Ap^\alpha x + p^\beta y \equiv p^\alpha(2Ax + p^{\beta-\alpha}By) \pmod{p^{n+\alpha}}.$$

As x runs over a complete residue system modulo $p^{n+\alpha}$, so does $2Ax + p^{\beta-\alpha}By$ for any fixed value of y . Therefore, with (1.4) and Lemma 2.1, (3.1) will simplify to the statement of the theorem.

Assume now that $\beta < \alpha$ and in particular this means $\beta = 0$ which in turn implies $(\Delta, p) = 1$. As $\alpha \leq n$, by Lemma 2.4, we see that the innermost sum of (3.1) is non-zero if and only if $y \equiv 0 \pmod{p^\alpha}$. In such an instance, along with Lemma 2.1, the sum indexed by x in (3.1) will be given by $p^\alpha \cdot G(SA; p^{n+\alpha})$. Hence, by modifying the index of the outermost sum in (3.1) by this congruence condition, the double sum in (3.1) will simplify to

$$(3.2) \quad \frac{1}{p^\alpha} \cdot G(SA; p^{n+\alpha}) \sum_{\substack{y=0 \\ y \equiv 0 \pmod{p^\alpha}}}^{p^{n+\alpha}-1} e\left(\frac{S(4A)^{-1}\Delta y^2}{p^{n+\alpha}}\right).$$

Observe that by Corollary 2.1, we have

$$(3.3) \quad \begin{aligned} \frac{1}{p^\alpha} G(SA; p^{n+\alpha}) &= \left(\frac{SA}{p}\right)^{n+\alpha} \iota\left(\frac{p^{n+\alpha}-1}{2}\right)^2 p^{\frac{n-\alpha}{2}} = \left(\frac{SA}{p}\right)^{n-\alpha} \iota\left(\frac{p^{n-\alpha}-1}{2}\right)^2 p^{\frac{n-\alpha}{2}} \\ &= G(SA; p^{n-\alpha}). \end{aligned}$$

As $\alpha \leq n$, we may use Lemma 2.2 to simplify the sum indexed by y in (3.2). Thus, with (3.3) and Lemma 2.1, (3.2) will simplify to $G(SA; p^{n-\alpha}) \cdot G(SA\Delta; p^{n+\alpha})$.

We now suppose that $p = 2$. If $\alpha = n$, then $\beta = 0$ so that b is odd. Additionally, c is even, and so the statement of the theorem will agree with Lemma 2.5 for all $n \geq 1$. Thus, we may assume without loss of generality that $\alpha < n$. Similar to the above, with (1.2) and Corollary 2.2, we deduce that $G(a, b, c; S; 2^n)$ is given by

$$(3.4) \quad \frac{1}{2^{2(\alpha+2)}} \sum_{y=0}^{2^{n+\alpha+2}-1} e\left(\frac{SA^{-1}\Delta y^2}{2^{n+\alpha+2}}\right) \sum_{x=0}^{2^{n+\alpha+2}-1} e\left(\frac{SA^{-1}(2^{\alpha+1}Ax + 2^\beta By)^2}{2^{n+\alpha+2}}\right).$$

If $\alpha + 1 \leq \beta$, then we can extract a common factor of $2^{\alpha+1}$ as before so that with (1.4) and Lemma 2.1, (3.4) will simplify to

$$\begin{aligned} &\frac{1}{2^{2(\alpha+2)}} \cdot G(SA\Delta; 2^{n+\alpha+2}) \cdot G(SA2^{2(\alpha+1)}; 2^{n+\alpha+2}) \\ &= \frac{1}{4} \cdot G(SA\Delta; 2^{n+\alpha+2}) \cdot G(SA; 2^{n-\alpha}). \end{aligned}$$

Suppose instead that $\beta < \alpha + 1$, so that we have $\beta = 0$ and Δ odd. We look to evaluate the innermost sum in (3.4). If $\alpha + 2 \leq n$, by Lemma 2.4, we have that (3.4) simplifies to

$$(3.5) \quad \frac{1}{2^{\alpha+3}} \cdot G(SA; 2^{n+\alpha+2}) \sum_{\substack{y=0 \\ y \equiv 0 \pmod{2^\alpha}}}^{2^{n+\alpha+2}-1} e\left(\frac{SA^{-1}\Delta y^2}{2^{n+\alpha+2}}\right).$$

Subsequently, as $\alpha < n$, by Lemma 2.2, (3.5) will simplify to

$$(3.6) \quad \frac{1}{2^{\alpha+3}} \cdot G(SA; 2^{n+\alpha+2}) \cdot G(SA\Delta; 2^{n+\alpha+2}) = \frac{1}{4} \cdot G(SA; 2^{n-\alpha}) \cdot G(SA\Delta; 2^{n+\alpha+2}),$$

where we have simplified with Corollary 2.1 and Lemma 2.1 as necessary.

Thus, suppose now that $\alpha + 1 = n$ and observe that we cannot use Lemma 2.4 in this case. If $n = 1$, then a is odd and hence

$$\begin{aligned} G(a, b, c; S; 2) &= \sum_{x,y=0}^1 e\left(\frac{S(ax + bxy + cy)}{2}\right) = 1 + (-1)^a + (-1)^c + (-1)^{a+b+c} \\ &= (-1)^c(1 + (-1)^{b+1}), \end{aligned}$$

which agrees with the statement of the theorem. Otherwise, if $\alpha + 1 = n > 1$ we have $\beta = 0$, so that

$$(3.7) \quad \begin{aligned} G(a, b, c; S; 2^n) &= \sum_{x,y=0}^{2^n-1} e\left(\frac{S(2^{n-1}Ax^2 + Bxy + cy^2)}{2^n}\right) \\ &= \sum_{y=0}^{2^n-1} e\left(\frac{Scy^2}{2^n}\right) \sum_{x=0}^{2^n-1} (-1)^x e\left(\frac{SBxy}{2^n}\right). \end{aligned}$$

The sum indexed by x in (3.7) can be written as

$$(3.8) \quad \begin{aligned} \sum_{\substack{x=0 \\ x \text{ even}}}^{2^n-1} e\left(\frac{SBxy}{2^n}\right) - \sum_{\substack{x=0 \\ x \text{ odd}}}^{2^n-1} e\left(\frac{SBxy}{2^n}\right) &= 2 \sum_{\substack{x=0 \\ x \text{ even}}}^{2^n-1} e\left(\frac{SBxy}{2^n}\right) - \sum_{x=0}^{2^n-1} e\left(\frac{SBxy}{2^n}\right) \\ &= 2 \sum_{\substack{x=0 \\ y \equiv 0 \pmod{2^{n-1}}}}^{2^{n-1}-1} 1 - \sum_{\substack{x=0 \\ y \equiv 0 \pmod{2^n}}}^{2^n-1} 1. \end{aligned}$$

By assumption, we have $2^\alpha \mid c$ so we may write $c \equiv c_1 2^\alpha \pmod{2^n}$ for some integer c_1 . Hence, $e\left(\frac{Scy^2}{2^n}\right) = (-1)^{c_1 y}$. Thus, together with (3.8), breaking up the sum in (3.7) according to the parity of y yields

$$(3.9) \quad \begin{aligned} G(a, b, c; S; 2^n) &= \sum_{\substack{y=0 \\ y \text{ even}}}^{2^n-1} \left(2 \sum_{\substack{x=0 \\ y \equiv 0 \pmod{2^{n-1}}}}^{2^{n-1}-1} 1 - \sum_{\substack{x=0 \\ y \equiv 0 \pmod{2^n}}}^{2^n-1} 1 \right) \\ &\quad + (-1)^{c_1} \sum_{\substack{y=0 \\ y \text{ odd}}}^{2^n-1} \left(2 \sum_{\substack{x=0 \\ y \equiv 0 \pmod{2^{n-1}}}}^{2^{n-1}-1} 1 - \sum_{\substack{x=0 \\ y \equiv 0 \pmod{2^n}}}^{2^n-1} 1 \right). \end{aligned}$$

As $n \geq 2$, the second term of (3.9) vanishes, and we're left with

$$\begin{aligned}
 G(a, b, c; S; 2^n) &= \sum_{y=0}^{2^{n-1}-1} \left(2 \sum_{\substack{x=0 \\ y \equiv 0 \pmod{2^{n-2}}}}^{2^{n-1}-1} 1 - \sum_{\substack{x=0 \\ y \equiv 0 \pmod{2^{n-1}}}}^{2^n-1} 1 \right) \\
 &= 2 \sum_{y=0}^{2^{n-1}-1} \sum_{\substack{x=0 \\ y \equiv 0 \pmod{2^{n-1}}}}^{2^{n-1}-1} 1 - \sum_{y=0}^{2^{n-1}-1} \sum_{\substack{x=0 \\ y \equiv 0 \pmod{2^{n-1}}}}^{2^{n-1}-1} 1 \\
 &= 2^{n+1} - 2^n = 2^n,
 \end{aligned}$$

which agrees with the statement of the theorem. \square

We observe that for p odd, Theorem 3.1 agrees with Lemma 2.5 if $\alpha = n$. First, note that $\alpha > 0$ implies $\beta = 0$ and so Δ is coprime to p . Thus, by Corollary 2.1, the statement of Theorem 3.1 simplifies to

$$G(SA; p^{n-\alpha}) \cdot G(SA\Delta; p^{n+\alpha}) = G(SA\Delta; p^{2n}) = p^n.$$

Continuing in this manner, we have the following corollary.

Corollary 3.1. *Let p be a prime, $n \in \mathbb{N}$, $S \in \mathbb{Z}$ coprime to p and let $a, b, c \in \mathbb{Z}$ be as in (1.9), namely*

$$(a, b, c) = 1, \quad a \equiv p^\alpha A \pmod{p^n}, \quad b \equiv p^\beta B \pmod{p^n}, \quad c \equiv 0 \pmod{p^\alpha},$$

where $A, B \in \mathbb{Z}$ satisfy $p \nmid AB$, and $\alpha, \beta \in \mathbb{N}_0$. We recall our convention that if $p^n \mid a$, then we set $\alpha = n$ and $A = 1$. We also recall that $\Delta := 4ac - b^2$. We write

$$\begin{cases} \Delta \equiv p^\delta D \pmod{p^{n+\alpha}} & \text{if } p \text{ is odd} \\ \Delta \equiv 2^\delta D \pmod{2^{n+\alpha+2}} & \text{if } p = 2, \end{cases}$$

where $D \in \mathbb{Z}$ satisfies $p \nmid D$, and $\delta \in \mathbb{N}_0$.

If p is odd, we have

$$G(a, b, c; S; p^n) = p^{n+\frac{\delta}{2}} \left(\frac{SA}{p} \right)^\delta \left(\frac{D}{p} \right)^{n+\alpha+\delta} \left(\frac{-1}{p} \right)^{(n+\alpha)(\delta+1)} i^{\left(\frac{p^\delta-1}{2} \right)^2}.$$

If $p = 2$ and $\alpha + 1 < n$, we have

$$G(a, b, c; S; 2^n) = \begin{cases} 2^{\frac{3n+\alpha}{2}} \left(\frac{2}{SA} \right)^\delta (1 + i^{SA}) & \text{if } \delta = n + \alpha + 2 \\ 0 & \text{if } \delta = n + \alpha + 1 \\ 2^{n+\frac{\delta}{2}} \left(\frac{2}{SA} \right)^\delta \left(\frac{2}{D} \right)^{n+\alpha+\delta} i^{SA \left(\frac{D+1}{2} \right)^2} & \text{if } \delta \leq n + \alpha. \end{cases}$$

If $p = 2$ and $\alpha + 1 \geq n$, we have

$$G(a, b, c; S; 2^n) = \begin{cases} 2^n & \text{if } \alpha + 1 \geq n > 1 \\ (-1)^c(1 + (-1)^{b+1}) & \text{if } \alpha + 1 \geq n = 1. \end{cases}$$

Proof. Suppose p is odd. From Theorem 3.1, (1.4) and Corollary 2.1, we have

$$\begin{aligned} G(a, b, c; S; p^n) &= G(SA; p^{n-\alpha}) \cdot G(SAp^\delta D; p^{n+\alpha}) \\ &= \begin{cases} p^{n+\alpha} \cdot G(SA; p^{n-\alpha}) & \text{if } \delta = n + \alpha \\ p^\delta \cdot G(SA; p^{n-\alpha}) \cdot G(SAD; p^{n+\alpha-\delta}) & \text{if } \delta < n + \alpha \end{cases} \\ (3.10) \quad &= \begin{cases} p^{\frac{3n+\alpha}{2}} \left(\frac{SA}{p}\right)^{n+\alpha} i\left(\frac{p^{n+\alpha}-1}{2}\right)^2 & \text{if } \delta = n + \alpha \\ p^{n+\frac{\delta}{2}} \left(\frac{SA}{p}\right)^\delta \left(\frac{D}{p}\right)^{n+\alpha+\delta} i\left(\frac{p^{n+\alpha}-1}{2}\right)^2 i\left(\frac{p^{n+\alpha+\delta}-1}{2}\right)^2 & \text{if } \delta < n + \alpha. \end{cases} \end{aligned}$$

Observe that the cases in (3.10) will agree when $\delta = n + \alpha$. Subsequently, we have

$$\begin{aligned} (3.11) \quad i\left(\frac{p^{n+\alpha}-1}{2}\right)^2 i\left(\frac{p^{n+\alpha+\delta}-1}{2}\right)^2 &= \begin{cases} \left(\frac{-1}{p}\right)^{n+\alpha} & \text{if } \delta \text{ even} \\ i\left(\frac{p^\delta-1}{2}\right)^2 & \text{if } \delta \text{ odd} \end{cases} \\ &= \left(\frac{-1}{p}\right)^{(n+\alpha)(\delta+1)} i\left(\frac{p^\delta-1}{2}\right)^2. \end{aligned}$$

Hence, with (3.10) and (3.11) we may deduce the statement of the corollary.

Suppose now $p = 2$ and $\alpha + 1 < n$. Note that this implies $n \geq 2$. By Theorem 3.1, (1.4) and Corollary 2.1, we have

$$\begin{aligned} G(a, b, c; S; 2^n) &= \frac{1}{4} \cdot G(SA; 2^{n-\alpha}) \cdot G(SA2^\delta D; 2^{n+\alpha+2}) \\ &= \begin{cases} 2^{n+\alpha} \cdot G(SA; 2^{n-\alpha}) & \text{if } \delta = n + \alpha + 2 \\ 0 & \text{if } \delta = n + \alpha + 1 \\ 2^{\delta-2} \cdot G(SA; 2^{n-\alpha}) \cdot G(SAD; 2^{n+\alpha+2-\delta}) & \text{if } \delta \leq n + \alpha \end{cases} \\ (3.12) \quad &= \begin{cases} 2^{\frac{3n+\alpha}{2}} \left(\frac{2}{SA}\right)^{n+\alpha} (1 + i^{SA}) & \text{if } \delta = n + \alpha + 2 \\ 0 & \text{if } \delta = n + \alpha + 1 \\ 2^{n+\frac{\delta}{2}-1} \left(\frac{2}{SA}\right)^\delta \left(\frac{2}{D}\right)^{n+\alpha+\delta} (1 + i^{SA})(1 + i^{SAD}) & \text{if } \delta \leq n + \alpha. \end{cases} \end{aligned}$$

Depending on the residue class of D modulo 4, we have

$$(3.13) \quad (1 + i^{SA})(1 + i^{SAD}) = \begin{cases} 2i^{SA} & \text{if } D \equiv 1 \pmod{4} \\ 2 & \text{if } D \equiv 3 \pmod{4}. \end{cases}$$

Thus, with (3.12) and (3.13) we may deduce the statement of the corollary.

Finally the case $p = 2$ and $\alpha + 1 \geq n$ follows immediately from Theorem 3.1. \square

We note that the results of Theorem 3.1 and Corollary 3.1 agree with the results of Weber [6, p. 22] and Alaca, et al. [1, pp. 129-132].

4. EXAMPLES

We provide a few examples to illuminate our method.

Example 4.1. Suppose that $Q := Q(x, y) = x^2 + xy + y^2$, so that $a = b = c = 1$. Thus $M = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ is the symmetric integral matrix associated with Q , and $\Delta = 3$.

For $p > 3$, we take $A = 1$, $D = 3$ and $\alpha = \delta = 0$ in Corollary 3.1 to obtain

$$(4.1) \quad G(1, 1, 1; S; p^n) = p^n \left(\frac{-3}{p} \right)^n.$$

For $p = 3$, we take $A = 1$, $D = 1$, $\alpha = 0$ and $\delta = 1$ in Corollary 3.1 to obtain

$$(4.2) \quad G(1, 1, 1; S; 3^n) = 3^{\frac{2n+1}{2}} \left(\frac{S}{3} \right) i.$$

Finally, for $p = 2$, we assume for the sake of discussion that $n \geq 2$. We take $A = 1$, $D = 3$ and $\alpha = \delta = 0$ in Corollary 3.1 to obtain

$$(4.3) \quad G(1, 1, 1; S; 2^n) = 2^n \left(\frac{2}{3} \right)^n = (-1)^n 2^n.$$

Alternatively, we can use Theorem 3.1 and subsequently Theorem 2.1 to obtain the same results.

We note that (4.1) and (4.2) are given by Corollary 2.1(i) [1, p. 137], and (4.3) agrees with Corollary 3.2(i) [1, p. 151] of Alaca, et al.

Example 4.2. Suppose that $Q := Q(x, y) = 3x^2 + xy + 3y^2$, so that $a = c = 3$ and $b = 1$. Thus $M = \begin{pmatrix} 6 & 1 \\ 1 & 6 \end{pmatrix}$ is the symmetric integral matrix associated with Q , and $\Delta = 35$.

For $p > 7$, we take $A = 3$, $D = 35$ and $\alpha = \delta = 0$ in Corollary 3.1 to obtain

$$G(3, 1, 3; S; p^n) = p^n \left(\frac{-35}{p} \right)^n.$$

For $p = 7$, we take $A = 3$, $D = 5$, $\alpha = 0$ and $\delta = 1$ in Corollary 3.1 to obtain

$$G(3, 1, 3; S; 7^n) = 7^{\frac{2n+1}{2}} \left(\frac{3S}{7} \right) \left(\frac{5}{7} \right)^{n+1} i = (-1)^n 7^n \left(\frac{S}{7} \right) \sqrt{-7}.$$

For $p = 5$, we take $A = 3$, $D = 7$, $\alpha = 0$ and $\delta = 1$ in Corollary 3.1 to obtain

$$G(3, 1, 3; S; 5^n) = 5^{\frac{2n+1}{2}} \left(\frac{3S}{5} \right) \left(\frac{7}{5} \right)^{n+1} = (-1)^n 5^n \left(\frac{S}{5} \right) \sqrt{5}.$$

Finally, for $p = 2$, and assuming $n \geq 2$, we take $A = 3$, $D = 35$ and $\alpha = \delta = 0$ in Corollary 3.1 and we conclude that

$$G(3, 1, 3; S; 2^n) = 2^n \left(\frac{2}{35} \right)^n = (-1)^n 2^n.$$

Alternatively, we can use Theorem 3.1 and Theorem 2.1 to obtain the same results.

5. REMARKS

It is straightforward to deduce the following theorem using our method.

Theorem 5.1. *Let $k \in \mathbb{N}$ be odd, and $a, b, c \in \mathbb{Z}$ be as in (1.9). If $(a\Delta, k) = 1$, then*

$$G(a, b, c; S; k) = \left(\frac{-\Delta}{k} \right) \cdot k.$$

Proof. Using the approach of Theorem 3.1, we obtain

$$\begin{aligned} G(a, b, c; S; k) &= G(Sa; k) \cdot G(Sa\Delta; k) \\ &= \left(\frac{Sa}{k} \right) i^{\left(\frac{k-1}{2}\right)^2} k^{\frac{1}{2}} \cdot \left(\frac{Sa\Delta}{k} \right) i^{\left(\frac{k-1}{2}\right)^2} k^{\frac{1}{2}} \\ &= \left(\frac{-\Delta}{k} \right) \cdot k, \end{aligned}$$

which completes the proof. □

We plan to show in an upcoming paper how we may use our method to give an explicit evaluation of a quadratic form Gauss sum in n variables. We also plan on demonstrating how we may use our evaluation of the double Gauss sum $G(a, b, c; S; p^n)$ to determine an explicit formula for the number of solutions to the congruence $ax^2 + bxy + cy^2 \equiv k \pmod{p^n}$ for a given integer k .

ACKNOWLEDGMENTS

The research of Şaban Alaca was supported by a Discovery Grant from the Natural Sciences and Engineering Research Council of Canada (RGPIN-2015-05208).

REFERENCES

- [1] A. Alaca, Ş. Alaca and K. S. Williams, Double Gauss Sums, *J. Comb. Number Theory* **6** (2014), 127-153.
- [2] B. C. Berndt, R. J. Evans and K. S. Williams, *Gauss and Jacobi Sums*, Canad. Math. Soc. Series of Monographs and Advanced Texts, Wiley, New York, 1998.
- [3] L. E. Dickson, *Modern Algebraic Theories*, B. H. Sanborn & Co., Chicago, 1926.
- [4] C. F. Gauss, Summatio Quarundam Serierum Singularium, *Comment. Soc. Reg. Sci. Gottingensis* **1**(1811).
- [5] C. Jordan, Sur les sommes de Gauss à plusieurs variables, *Comptes rendus hebdomadaires des séances de l'Académie des sciences* **73** (1871), 1316-1319.

- [6] H. Weber, Über die mehrfachen Gaussischen Summen, *J. Reine Angew. Math.* **74**(1872), 14-56.

Şaban Alaca and Greg Doyle
School of Mathematics and Statistics
Carleton University, Ottawa
Ontario, K1S 5B6, Canada

SabanAlaca@cunet.carleton.ca
gdoyle@math.carleton.ca